CLAIMS

What is claimed is:

1. A method for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

(a) initiating a risk assessment scan on a target from a remote source utilizing a network;

(b) determining whether the risk assessment scan involves an intermediate device coupled between the target and the remote source;

(c) receiving results of the risk assessment scan from the target utilizing the network; and

(d) notifying an administrator if it is determined that the risk assessment scan involves the intermediate device.

2. The method as recited in claim 1, wherein the intermediate device includes a router.

3. The method as recited in claim 1, wherein the intermediate device includes a proxy server.

3. The method as recited in claim 1, wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device.

4. The method as recited in claim 3, wherein at least one of the procedures includes determining a port list associated with the risk assessment scan.

5. The method as recited in claim 4, wherein the at least one of the procedures further includes determining whether a value of a flag is different for communication attempts using at least two ports on the port list.

6. The method as recited in claim 5, wherein the flag includes an ip_ttl flag.

7. The method as recited in claim 5, wherein the flag includes a tcp_win flag.

8. The method as recited in claim 5, wherein the communications include connection attempts between the remote source and the target utilizing the network.

9. The method as recited in claim 5, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the value of the flag is different for the communication attempts using the at least two ports on the port list.

10. The method as recited in claim 3, wherein at least one of the procedures includes transmitting a first request for content to the target utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network.

11. The method as recited in claim 10, wherein the cached content is requested from the target utilizing a via tag.

12. The method as recited in claim 10, wherein the at least one of the procedures further includes analyzing responses to the first and second requests.

13. The method as recited in claim 12, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis.

14. The method as recited in claim 13, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different.

15. The method as recited in claim 3, wherein at least one of the procedures includes transmitting a request without specifying a host header value.

16. The method as recited in claim 15, wherein the at least one of the procedures further includes identifying an error message in response to the request.

17. The method as recited in claim 16, wherein the at least one of the procedures includes indicating that the risk assessment scan involves the intermediate device if the response includes the error message.

18. A computer program product for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

(a) computer code for initiating a risk assessment scan on a target from a remote source utilizing a network;

(b) computer code for determining whether the risk assessment scan involves an intermediate device coupled between the target and the remote source;

(c) computer code for receiving results of the risk assessment scan from the target utilizing the network; and

(d) computer code for notifying an administrator if it is determined that the risk assessment scan involves the intermediate device.

19. The computer program product as recited in claim 18, wherein the intermediate device includes a router.

20. The computer program product as recited in claim 18, wherein the intermediate device includes a proxy server.

21. The computer program product as recited in claim 18, wherein a plurality of procedures are utilized to determine whether the risk assessment scan involves the intermediate device.

22. The computer program product as recited in claim 21, wherein at least one of the procedures includes determining a port list associated with the risk assessment scan.

23. The computer program product as recited in claim 22, wherein the at least one of the procedures further includes determining whether a value of a flag is different for communication attempts using at least two ports on the port list.

24. The computer program product as recited in claim 23, wherein the flag includes an ip_ttl flag.

25. The computer program product as recited in claim 23, wherein the flag includes a tcp_win flag.

26. The computer program product as recited in claim 23, wherein the communications include connection attempts between the remote source and the target utilizing the network.

27. The computer program product as recited in claim 23, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the value of the flag is different for the communication attempts using the at least two ports on the port list.

28. The computer program product as recited in claim 21, wherein at least one of the procedures includes transmitting a first request for content to the target

utilizing the network, and transmitting a second request for a cached version of the content to the target utilizing the network.

29. The computer program product as recited in claim 28, wherein the cached content is requested from the target utilizing a via tag.

30. The computer program product as recited in claim 28, wherein the at least one of the procedures further includes analyzing responses to the first and second requests.

31. The computer program product as recited in claim 30, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device based on the analysis.

32. The computer program product as recited in claim 31, wherein the at least one of the procedures further includes indicating that the risk assessment scan involves the intermediate device if the responses to the requests are different.

33. The computer program product as recited in claim 21, wherein at least one of the procedures includes transmitting a request without specifying a host header value.

34. The computer program product as recited in claim 33, wherein the at least one of the procedures further includes identifying an error message in response to the request.

35. The computer program product as recited in claim 34, wherein the at least one of the procedures includes indicating that the risk assessment scan involves the intermediate device if the response includes the error message.

36. A system for detecting modifications to risk assessment scanning caused by an intermediate device, comprising:

(a) logic for initiating a risk assessment scan on a target from a remote source utilizing a network;

(b) logic for determining whether the risk assessment scan involves an intermediate device coupled between the target and the remote source;

(c) logic for receiving results of the risk assessment scan from the target utilizing the network; and

(d) logic for notifying an administrator if it is determined that the risk assessment scan involves the intermediate device.

37. A method for detecting modifications to risk assessment scanning caused by a proxy server, comprising:

(a) initiating a risk assessment scan on a target from a remote source utilizing a network;

(b) executing a plurality of procedures to determining whether the risk assessment scan involves a proxy server coupled between the target and the remote source;

(c) said procedures utilizing a plurality of parameters selected from the group consisting of an ip_ttl flag, a tcp_win flag, a via tag, and a host header value;

(d) receiving results of the risk assessment scan from the target utilizing the network;

(e) flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source; and

(f) notifying an administrator if the results of the risk assessment scan are flagged.

38. A computer program product for detecting modifications to risk assessment scanning caused by a proxy server, comprising:

(a) computer code for initiating a risk assessment scan on a target from a remote source utilizing a network;

(b) computer code for executing a plurality of procedures to determining whether the risk assessment scan involves a proxy server coupled between the target and the remote source;

(c) said procedures utilizing a plurality of parameters selected from the group consisting of an ip_ttl flag, a tcp_win flag, a via tag, and a host header value;

(d) computer code for receiving results of the risk assessment scan from the target utilizing the network;

(e) computer code for flagging the results of the risk assessment scan if at least one of the procedures indicates that the risk assessment scan involves a proxy server coupled between the target and the remote source;

(f) computer code for notifying an administrator if the results of the risk assessment scan are flagged.